¿PRIVACIDAD, DATOS Y UN ESTADO VIGILANTE EN TIEMPOS DE PANDEMIA?

Cifras y Conceptos*

Mayo 12 de 2020

Como ha dicho Yuval Harari, "en esta pandemia la información de buena calidad es más útil que el confinamiento" (2020). Por ello, todos los países se han visto en la imperiosa necesidad de contar con mejores datos que permitan entender en el menor tiempo posible la naturaleza del fenómeno.

Afortunadamente, hoy existen las tecnologías que facilitan rastrear las cadenas de contagio y acopiar información para atender a las personas más necesitadas e identificar a las personas que requieren ayudas sociales. Para lograr estos objetivos se requieren datos personales y privados de la población que en Colombia estaban protegidos antes de la pandemia por las normas de *habeas data*.

El acceso de los gobiernos a información personal y sensible de la ciudadanía puede no ser respetuoso de la protección de datos, violar la privacidad de las personas y abrir la puerta a un sistema de vigilancia abusiva sobre la población civil. Nos enfrentamos, entonces, a un dilema:

- **¿Estamos dispuestos a darle nuestros datos sensibles al gobierno para que sea más efectiva la lucha contra el coronavirus?**
- **¿Confiamos en el manejo que darán a esta información privada las autoridades?**

MEDIDAS DEL GOBIERNO DE COLOMBIA

El gobierno ha tomado al menos tres medidas durante la emergencia sanitaria con las que la protección de los datos y la privacidad puede estar en alto riesgo. Ellas, básicamente, permiten que las entidades públicas tengan acceso a información personal de los ciudadanos sin su autorización.

1. Circular Externa 1 de 2020 de la Superintendencia de Industria y Comercio
Informa a los operadores de telefonía móvil que la ley los autoriza a suministrar datos personales **sin autorización del titular** a entidades públicas como el Departamento Nacional de Planeación, con el fin de enfrentar el coronavirus. Esta circular se basa en el artículo 10 de la Ley de Protección de Datos Personales, que establece que las emergencias médicas y sanitarias son uno de los casos en los que no es necesaria la autorización del titular para el tratamiento de sus datos.

2. Artículo 3 del Decreto 458 de 2020: tratamiento de la información estadística
Dice que el DANE deberá suministrar la información de censos y encuestas a las entidades del Estado que lo soliciten para implementar medidas de control del coronavirus sin la reserva legal de la Ley 79 de 1993. Esto acaba la promesa de confidencialidad estadística permitiéndole a la entidad entregar, por primera vez en su larga historia, información desagregada a nivel de individuos, sin el consentimiento de las personas.

CIFRAS & CONCEPTOS
INFORMACIÓN INTELIGENTE®

* César Caballero con la colaboración de Helena Hernández y comentarios de Miguel Ángel León y Eduardo Freire.

3. CoronApp

Es la aplicación del gobierno para detectar y monitorear casos de Coronavirus, focalizar puntos de contagio y controlar la expansión del virus. La aplicación pide para registrarse nombres y apellidos, tipo y número de documento y número de celular. También solicita permiso para acceder a la ubicación. Antes pedía acceder al bluetooth, pero en la actualización (27 de abril) se eliminó esta solicitud.

El gobierno afirma que toda la información que guarde la aplicación estará encriptada y protegida por la Ley de Habeas Data. De acuerdo con MinTic, "el análisis de la información se realiza de forma 100 % anónima. En algunos casos, se podrá compartir información a las autoridades de salud para el cuidado de los ciudadanos".

Los términos y condiciones (T&C) de la aplicación dicen que el tratamiento de los datos tiene diez objetivos distintos y se menciona que "se podrá suministrar información a las entidades públicas o administrativas que en el ejercicio de sus funciones legales así lo requieran".

Según MinTic, en un futuro cercano, la aplicación será un pasaporte de movilidad. "Serviría como un soporte del permiso de transitar por las calles en los casos de excepción y también como un mecanismo para mostrar cuándo se realizó el último control".

Algunos funcionarios encargados del tema han manifestado que existen todas las seguridades posibles y que su uso será sólo en el marco del Sigivila y únicamente por parte del INS. No obstante, los decretos dicen otra cosa.

RIESGOS DE LAS DECISIONES EN LA EMERGENCIA

Todos los países se enfrentan a decisiones sobre cómo utilizar la tecnología y cómo manejar la privacidad de los datos en medio de la emergencia. Algunos riesgos de estas estrategias son:

- La pandemia podría normalizar el uso de instrumentos de vigilancia masiva, como cámaras con reconocimiento facial y de temperatura en lugares públicos, acceso del gobierno a la geolocalización y a la señal de bluetooth de los celulares de los ciudadanos, etc.
- "Aumentar la vigilancia para combatir la pandemia ahora podría abrir permanentemente las puertas a formas de espionaje más invasivas más adelante" (The New York Times, 2020).
- Las medidas de excepción tomadas bajo el estado de emergencia podrían quedarse más tiempo con cualquier excusa (otro virus, por ejemplo).
- Estas medidas extraordinarias abren el camino al autoritarismo, pues restringen libertades y derechos individuales y se toman con más poder del habitual. Hay pocas garantías de que los gobiernos no abusen de las facultades adicionales que ahora tienen y que solo las usen para enfrentar la pandemia. La democracia y el equilibrio de poderes están en riesgo.
- "En la sociedad altamente cableada de Corea del Sur, las multitudes de Internet explotaron los datos de pacientes divulgados por el sitio del gobierno para identificar a las personas por su nombre y acosarlas" (The New York Times, 2020).

Así como las situaciones extraordinarias requieren medidas extraordinarias, las medidas requieren una supervisión mayor, tanto legal como técnica.

Es necesario poner límites a lo que realmente se necesita y particularmente tener todas las salvaguardias para evitar abusos con esta información.

¿CONFIAMOS EN UN ESTADO VIGILANTE?

La más reciente encuesta de Cifras y Conceptos encontró que el 71% de las personas no confía en la información del gobierno nacional. Esta semana revivió un escándalo adicional de seguimientos ilegales por parte del Ejército Colombiano y de forma cotidiana se conocen casos de filtraciones de información reservada en manos de entidades públicas. La Fundación Karisma ha venido mostrando todas las posibles fallas de seguridad y muchas dudas sobre la aplicación Coronapp.

Por ello, es pertinente preguntarse no sólo por la conveniencia de estas medidas sino también por la capacidad de nuestro Estado para, una vez consolidada, darle un uso adecuado, protegido y dentro del marco legal a la información. Las tres medidas tomadas por el gobierno dejan muchas dudas que vale la pena plantear y que sean respondidas con claridad:

- ¿A qué entidades gubernamentales les compartirán información los operadores telefónicos, Coronapp y el DANE?
- ¿Por cuánto tiempo tendrán acceso a la información las entidades?
- ¿Qué pasará con la información cuando se acabe la emergencia?
- ¿Cuáles son los objetivos específicos de que se entreguen los datos y cómo ayudará a enfrentar la emergencia?
- ¿Cuáles entidades privadas, además de los operadores de telefonía móvil, entregarán datos personales sin autorización?
- ¿Qué otros datos está recolectando Coronapp además de los que piden para el registro y los que reportan los usuarios?
- ¿Qué significa que la aplicación vaya a ser un pasaporte de movilidad? ¿No podremos salir si no tenemos la aplicación descargada y activa? ¿Será obligatorio su uso?
- Uno de los puntos de la licencia del DANE afirma que “El contenido de la información de las bases de datos podrá ser reproducido o distribuido sin modificaciones para los fines establecidos en el artículo 3 del Decreto 458 de 2020”. ¿La información a quién se le podrá distribuir y cómo se podrá reproducir?

Finalmente, y considerando la baja credibilidad que hoy tiene el Estado en materia de información y los escándalos por vulneración de derechos y manejo indebido de la información y la privacidad por parte del Ejército:

¿Se sentiría usted tranquilos con toda su información privada en manos de ellos?

Referencias

- Harari, Yuval Noah. (Marzo 15 de 2020). In the Battle Against Coronavirus, Humanity Lacks Leadership. En https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/
- The New York Times. (Marzo 23 de 2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. En https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
- Fundación Karisma. (Mayo 9 de 2020). La Coronapp podría no servir y en cambio le estamos entregando nuestra privacidad. En https://lasillavacia.com/silla-llena/red-de-la-innovacion/la-coronapp-podria-no-servir-y-cambio-le-estamos-entregando